NOKIA

Smart Waste Solution

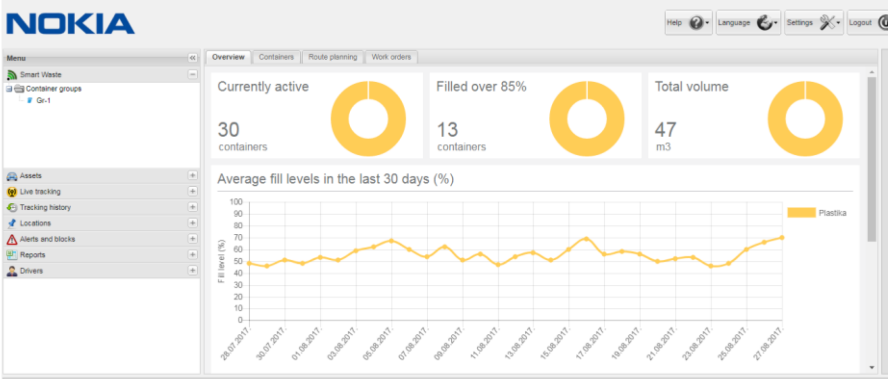
Smart Waste Overview

Customer Challenge

- Keeping cities clean & odor-free while optimizing operational efficiencies associated with waste management
- Need to safeguard against disease

Nokia Solution

- Multi-bin support (works with any receptacle)
- Optimal route generation
- Rugged sensor design
- Measurements - Fill Level
- Measurements - Temperature
- Measurements – Container position
- Automatic alarming
- Color codes fill levels depicting the capacity status



Currently active 30 containers

Filled over 85% 13 containers

Total volume 47 m3

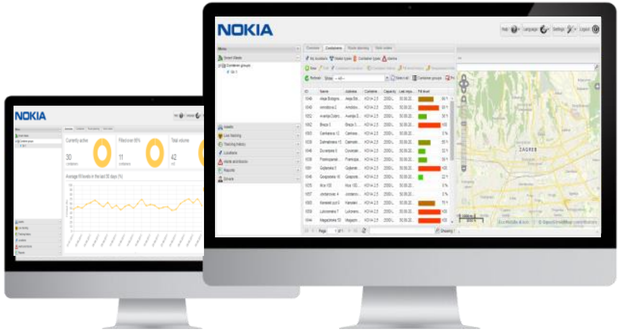
Average fill levels in the last 30 days (%)

Business Benefits

- Reduced labor
- Direct cost savings
- Reduced dumpster trips
- Increased utilization of assets
- Improved service
- Reduction of CO_2 emission

Smart Waste Solution Overview

- Remote fill level measuring of waste containers & auto alerting
- Optimization of collection and transport with proprietary analytics algorithms
- Solution Components
  - Wireless ultrasonic fill level monitoring sensor
  - Cellular connectivity (2G/3G, NB-IoT in roadmap)
  - Web oriented application for data management and analysis
  - Mobile application for driver navigation and work order management

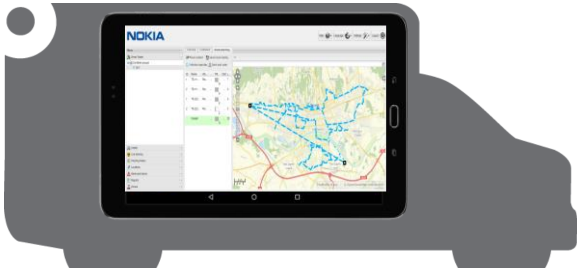


Central Operation

+

+

+



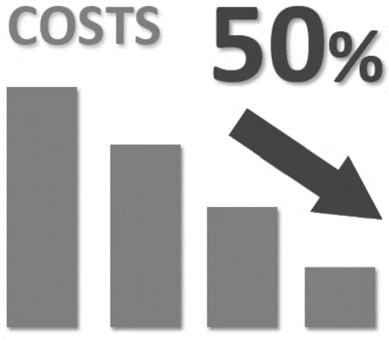
Sensor

T-Mobile Network

Nokia IoT Platform (IMPACT)

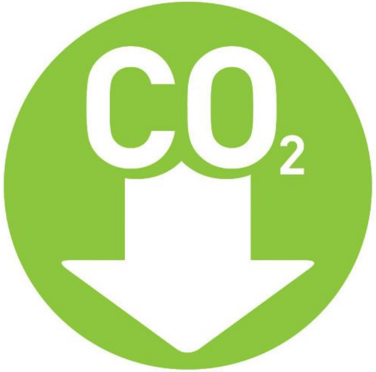
Field Operation

Key Benefits



Cost Reduction

The use of Smart Waste system provides up to 50% in direct cost savings in transport and logistics



Less CO2 Emission

Optimization of waste collection by reducing the number of collection runs which also reduces the amount of CO2 emissions.

Clean Environment

Timely and accurate information about each containers fill level prevents overfilling and contributes to nicer and cleaner environment.

Demo

http://209.202.115.189/MainDemos/2017/smartwaste/

IoT Security

Mission Critical Networks are Under Attack

3% of global mining, oil, gas companies hacked

Hackers use virus to steal £20 MILLION from UK bank accounts

MIRAI Bot DDoS attack ->1.2 million infected IoT devices

Hacker group Dragonfly 2.0 compromised OT networks of 2 utilities in the US and Europe

2014 2015 2016 2017

US Department of Energy hacked 150 times in four years

Ukrainian grid attack -> 250,000 people without power

Flight information screens in two Vietnam airports hacked

Global WannaCry attack -> 200,000+ endpoints; disturbance of services

Loss of revenue and compensations

Recovery and restoration costs

Potential lawsuits and penalties

Damage to brand reputation

"While many cyber defenses are improving in global enterprises, the number of bad actors is also growing rapidly. The breadth and depth of cyber threats and online vulnerabilities continues to grow
- especially with new Internet of Things (IoT) devices coming onto the market."

Dan Lohrmann on cybersecurity & infrastructure, Government Technology magazine, Dec. 2016

IoT Security Challenges

The ‘S’ in IoT stands for ‘Security’ OT vs IT

Long IoT Device Lifetime

High effort to update devices in the field.
Outdated security mechanisms needed for legacy devices.

Signaling Storms

There will be many IoT devices.
Normal IoT device signaling footprint will often be low.

Encryption power decreases over lifetime

→ Cracking of encryption in 5-10 years possible!

Anti-Malware support seldom available for 10+ years

→ Small quantities might not get any support!

Malware could increase device activity drastically

→ Networks can overload

→ Battery drain

Networks are not overprovisioned to cater for unexpected high loads

Roaming devices could jump between networks

→ Affects visited network and roaming interfaces

When a network goes down or locks out devices, they seek for connectivity

maintained IoT devices

How many users really care as long as it works?

Who updates the camera?

→ Vulnerable devices can be hijacked by attackers

Nobody will care about it as long as the camera works,...

Overlap of IT and OT

•Unintentional linkages are formed accidently over time

•Vulnerabilies are created

Security
Challenge?!

Types of Compromise for IoT

Data

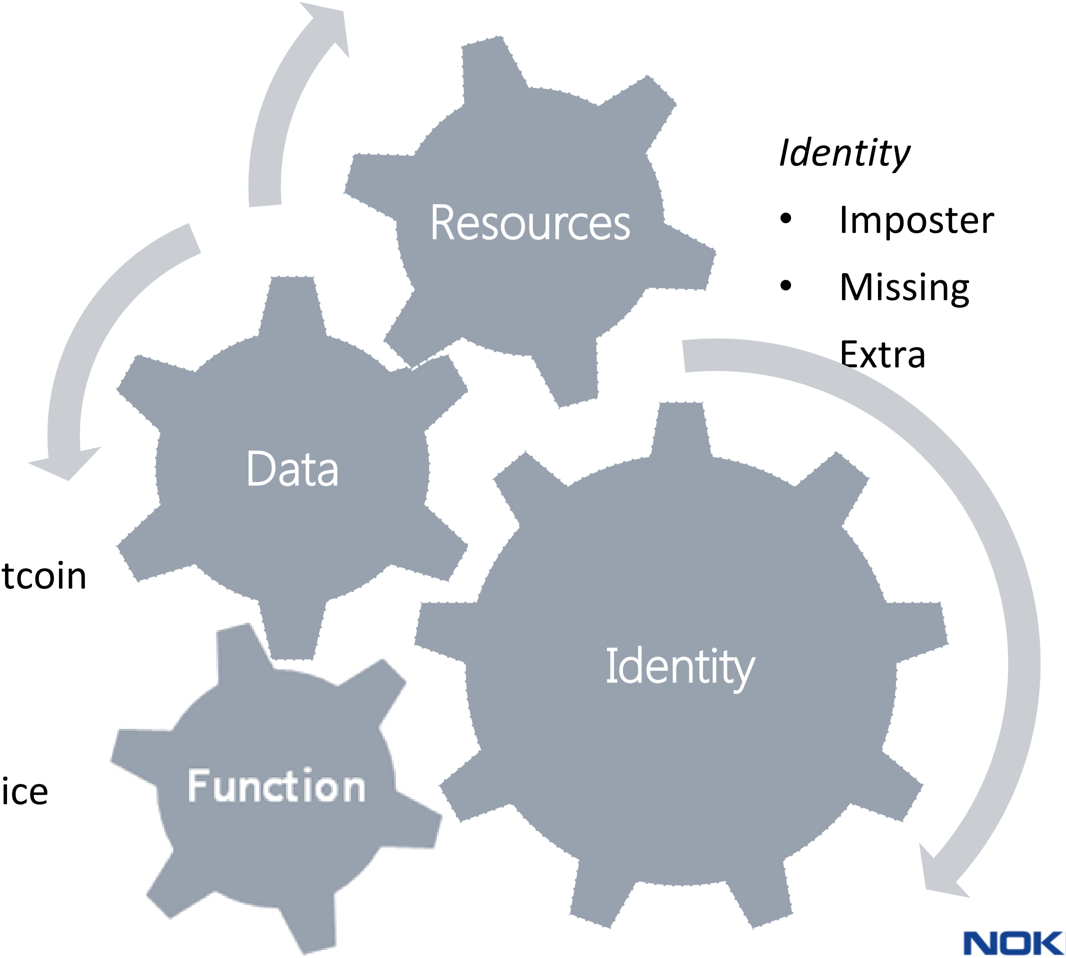
- Data exfiltration
- Data modification/corruption
- Data suppression
- Ransomware

Resources

- Theft of device resources for bitcoin mining or spambots

Function

- Disrupt the function of the service for business or political aims



Identity

- Imposter
- Missing
- Extra

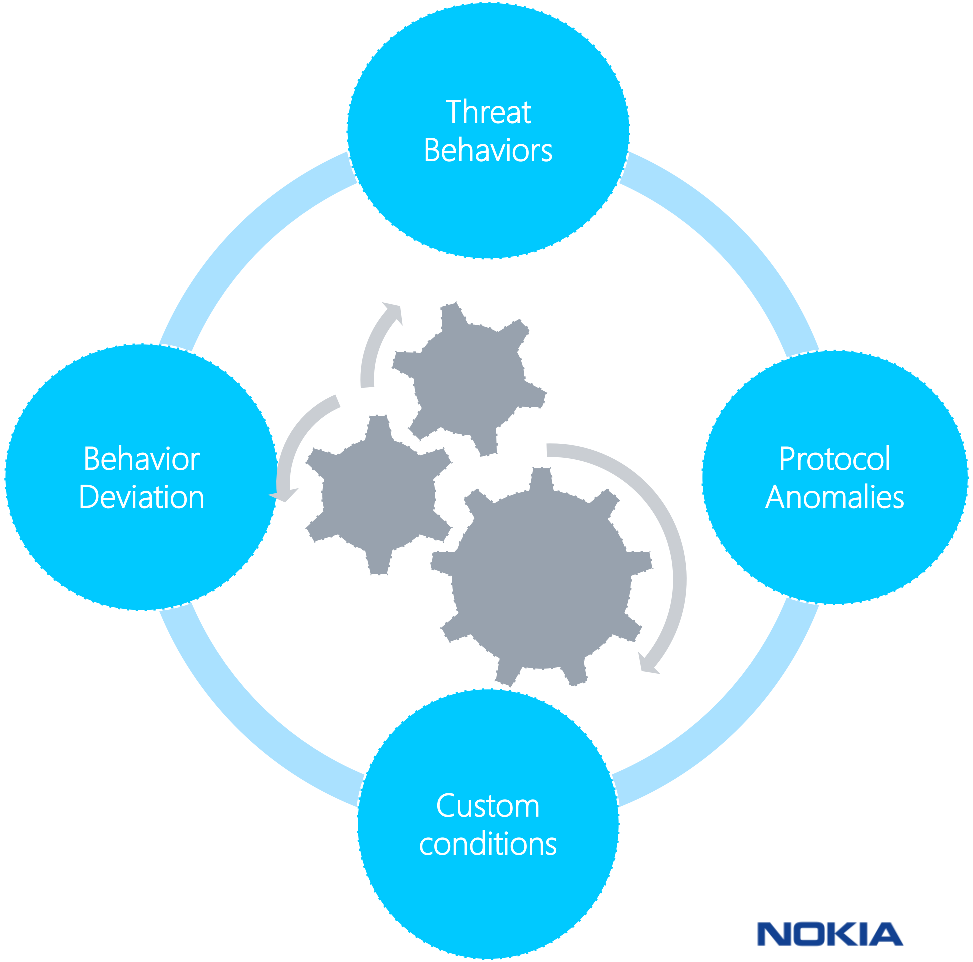
360 degrees of monitoring

1) **Malware/threat behavior** – exact match with a threat conditions

2) **Device profile anomalies** – not correct per approved profile

3) **Protocol anomalies** – even if not defined as a threat behavior (DNP3, Modbus)

4) **Custom conditions** – can be defined and expressed.



Recommended Best Practices

A Closer Look NERC CIP: 10 Standards, 30 Requirements

CIP-002	CIP-003	CIP-010	CIP-011
BES CYBER-SYSTEM IDENTIFICATION AND CATEGORIZATION	SECURITY MANAGEMENT CONTROLS	CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENT	INFORMATION PROTECTION
1. BSS CYBER SYSTEM IDENTIFICATION	1. CYBER SECURITY POLICY FOR HIGH/MED SYSTEMS	1. CONFIGURATION CHANGE MANAGEMENT	1. INFORMATION PROTECTION
2. REGULAR APPROVAL	2. CYBER SECURITY POLICY FOR LOW SYSTEMS	2. CONFIGURATION MONITOING	2. BES CYBER ASSET REUSE AND DISPOSAL
		3.VULNERABILITY ASSESSMENTS	

Privileged Account Management

- Implement access control policies
- Proactively secure privileged credentials
- Rotate admin credentials after each use
- Monitor privileged account usage to detect anomalies

Configuration Compliance Checking

- Develop and maintain baseline configurations
- Record deviations from baselines
- Update baseline configurations after a change
- Monitor the baseline configuration every 35 days

Scan for Malware

Secure Networking

- Encrypt communications with external routable connectivity

Nokia Helps Utilities Implement Best Practices

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009	CIP-010	CIP-011
BES CYBER-SYSTEM IDENTIFICATION AND CATEGORIZATION	SECURITY MANAGEMENT CONTROLS	TRAINING AND PERSONNEL SECURITY	ELECTRONIC SECURITY PERIMETER	PHYSICAL SECURITY OF BES CYBER SYSTEMS	SYSTEMS SECURITY MANAGEMENT	INCIDENT REPORTING AND RESPONSE PLANNING	RECOVERY PLANS FOR BES CYBER SYSTEMS	CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENT	INFORMATION PROTECTION
NETGUARD INTEGRITY AUDIT COMPLIANCE MANAGER	NETGUARD SECURITY MANAGEMENT CENTER (NSMC)	1. AWARENESS	1. ELECTRONIC SECURITY PERIMETER	NSMC	NSMC	NSMC	1. RECOVERY PLAN SPECIFICATIONS	NACM	NETGUARD DATA PROTECTION (NDP)
2. REGULAR APPROVAL	NSMC	2. TRAINING	NIAM	NSMC	2. SECURITY PATCH MANAGEMENT	2. INCIDENT RESPONSE PLAN IMPLEMENTATION AND TESTING	2. RECOVERY PLAN IMPLEMENTATION AND TESTING	NACM + NSMC	2. BES CYBER ASSET REUSE AND DISPOSAL
		3. PERSONNEL RISK ASSESSMENT PROGRAM	1.5 DETECTION OF MALICIOUS COMMUNICATION	3. MAINTENANCE AND TESTING PROGRAM	NIAM + NETGUARD AUDIT COMPLIANCE MANAGER (NACM)	3. INCIDENT RESPONSE PLAN REVIEW, UPDATE AND COMMUNICATIO	3. RECOVERY PLAN REVIEW, UPDATE AND COMMUNICATION	NSMC	
		NETGUARD IDENTITY ACCESS MANAGER (NIAM)	NETGUARD ENDPOINT SECURITY (NES)		NSMC				
		NIAM			5. SYSTEM ACCESS CONTROLS				

🟦 Products

🟨 Services

NOKIA